AFCEA PKI Roundtable
PKI Implementation Lessons Learned
(Service Perspective)
June 15, 2000

Robert Weilminster
weilminster.robert@hq.navy.mil
(703)601-1278

Agenda

- Where we are today
  - Infrastructure Perspective
  - User Perspective
- Lessons Learned

Infrastructure Perspective

- The Navy Department has deployed a Class 4 PKI to support DMS
  - Over 90 CAs at Multiple Security Levels
  - Have distributed over 42K Tokens
- Navy Class 3 LRA infrastructure is growing
  - About 100 LRAs currently established
  - Issuance of server certs significantly increasing to meet DoD milestone - over 500 issued
  - Relatively few individual certs issued - over 1700 identity and 1000 e-mail. Target audience is >800K
- Planning begun to convert to R2.0

User Perspective

- Several PKI Pilots are underway
  - NAVSUP Navy Acquisition and One Touch Supply - which is in process of converting to DoD PKI
  - Implementations of Medium Grade Services (MGS) at NAVSEA, SPAWAR and DON CIO
  - NAVSAFECEN Outlook Web Access in process of converting to DoD PKI
  - DON CIO smart card based network access
- Server SSL implementations are growing
- Several Client-Server implementations operational

Lessons Learned - DMS Perspective

- Distributed CA infrastructure is difficult to maintain
- Ensuring token and pin distribution in accordance with CP sometimes requires significant planning
- Archive requirements
- Application to multiple security levels
  - Separate Infrastructures
  - Token Issues
- CRL issuance/use & update
- Tactical implementation
  - Access to directory
  - Token replacement

Lessons Learned - DoD Medium Assurance

- **Obtaining certificates - process & renewal**
- **Length of certificate life - ability to specify**
- **Adequate user identification - foreign nationals**
- **Available uses for certificates - enabled apps**
- **Adequate training/documentation**
- **Enabling applications**
  - **E-Mail**
    - **As transparent as possible to user**
    - **Directory interaction**
    - **Certificate validity verification**
  - **Client-Server**
    - **PKI and SSL - performance impact**
    - **Certificate validity verification**